REMARKS/ARGUMENTS

The applicant would like to acknowledge, with thanks, the Office Action mailed December 28, 2006. This amendment and response is responsive to the Office Action mailed December 28, 2006. By this amendment, independent claims 1, 9 and 17 have been amended. Independent claims 1, 9 and 17 were amended to claim that the tunneling and authentication keys were established before the issuing of secured credentials. New dependent claims 25-27 provide for the hashing of the authorization key and the encryption key. This subject matter is not new matter as it is disclosed in the first full paragraph, lines 1-3, on page 11 of the specification.

I. Claim Rejections

Claims 1-5, 7, 9-13, 15, 17-21 and 23 stand rejected based on the U.S. Patent Publication No. 2002/0157021 A1 to Yokote (*hereinafter* Yokote). Claims 6, 8, 14, 16, 22 and 24 stand rejected as begin obvious based on the combination of Yokote and U.S. Patent Publication. 2002/022617 to Palekar et al. (hereinafter Palekar). For reasons that will now be set forth, claims independent claims 1, 9, and 17 as amended are not anticipated by Yokote.

Independent claims 1, 9, and 17 have been amended to recite that the tunneling key and authentication keys are verified to ensure the first and second parties possess the same authentication and encryption keys. Only when both of those keys are the same will secure credentials be provided to the peer by the authentication server. Verifying that the encryption and authentication keys are the same before issuing secure credentials combats a "man in the middle" attack.

By contrast, Yokote is primarily interested in a security association management scheme to ensure security synchronization between nodes, removing the association when they are not needed and updating security association when a mobile node roams to another agent (see abstract and par. 44). Yokote teaches using IPsec which teaches using a secured tunnel (see par. 48, lines 15-18 and also teaches performing an authentication between a node and an authentication server (see par. 48, lines 13-14). Yokote does not verify that the encryption and authentication keys are the same between both peers nor does Yokote hash any key material used to create the secured tunnel or to perform the subsequent authentication. Moreover, Yokote is

vulnerable to a "man in the middle" attack. Unlike Yokote, independent claims 1, 9, and 17 teach verifying the key material from both the secured channel and the authentication process.

Because Yokote does not teach all of the claim elements of amended independent claims 1, 9, and 17, they are not anticipated by Yokote. Claims 2-8, 10-16, and 18-24 depend directly from claims 1, 9, and 17 respectively and therefore contain each and every element of those claims, respectively.

The Examiner uses Palekar to teach Microsoft MS-CHAPv2 may be used in performing the authentication and to teach the step of provisioning public/private key pairs in accordance with Public Key Infrastructure (PKI), however, both of these teachings do not remedy the aforementioned deficiency. Claims 1, 9 and 17, by contrast, teach verifying the key material from the secured tunnel and authentication keys before issuing secured credentials to the peer.

Claims 2-8 and 25 are directly dependent from claim 1, and therefore contain each and every element of claim 1. Claims 10-16 and 26 are directly dependent from claim 9, and therefore contain each and every element of claim 9. Claims 18-24 and 27 are directly dependent from claim 17, and therefore contain each and every element of claim 17. Therefore, for the reasons already set forth for claims 1-27 are not obvious in view of Yokote and/or Palekar.

In addition to the reasons just set forth above, new claims 25-27 recite that the verifying process (or step) further comprises hashing the first party encryption key and authentication key to produce a first hash. In addition claims 25-27 recite hashing the second party encryption key and authentication key to produce a second hash. The verifying step further comprising verifying that the first and second hash are the same (e.g. match). Nothing in either Yokote and/or Pelekar teach or suggest hashing the authentication and encryption keys of the first and second parties and determining whether or not the hashes match. Thus, for the reasons just set forth, neither Yokote nor Pelekar, when taken alone or in combination do not teach or suggest every element of new claims 25-27.

Conclusion

For the reasons just set forth, applicant respectfully requests withdrawal of the rejections. The examiner is invited to contact the undersigned if there are any other matters to be discussed. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: March 5, 2007

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009